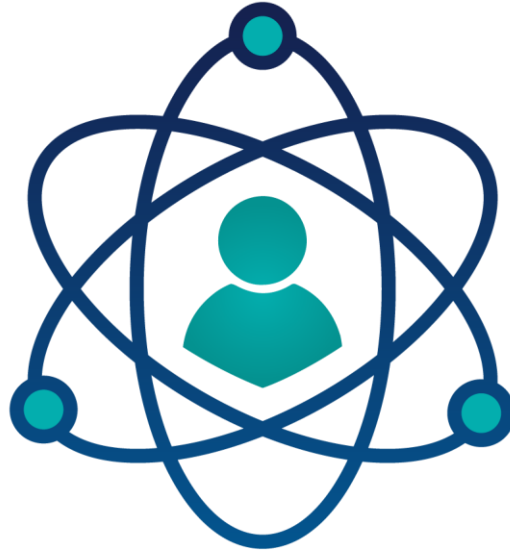Ecosystem for Services based on integrated Cross-sectorial Data Streams from multiple Cyber Physical Products and Open Data Sources

CROSS-CPP

CROSS-CPP

CROSS-CPP Ecosystem Policy Guidelines

Cross-CPP ecosystem Internal (Legal, Privacy, Consent) Policies Guides

Table of Contents

1. Introduction

The process/activity related Methodology Guidelines describes regulations in respect to the interaction between the key Cross-CPP Ecosystem Stakeholders with the Ecosystem, such as contractual and privacy/security issues, as well as update of reference data model regulations.

1.1. Purpose

The presented methodology guidelines cover legal, privacy and consent regulations for key processes/activities in respect to the actions/roles of the various stakeholders and their interaction required for the operation of the Cross-GPP Ecosystem.

1.2. Audience

The methodology guidelines are meant for all stakeholders of the Cross-CPP Ecosystem, as well as candidates planning to be a stakeholder.

1.3. Scope

The contents of the methodology guidelines will cover regulations in respect to the interaction between the various stakeholders.

Cross-CPP team does not take responsibility, when not following the instructions given in this guide.

If you find a regulation for which there is no content in this guide you can request it through: general-support@cross-cpp.eu.

1.4. Contact

Cross-CPP Project website: https://cross-cpp.eu

Cross-CPP Marketplace: https://datagora.eu

Marketplace support: marketplace-support@cross-cpp.eu

Context Monitoring and Extraction Module (CME): context-support@cross-cpp.eu.

Policy guidelines and in general: general-support@cross-cpp.eu

2. Structure of the Guide

In reference to methodology concept outlined in D1.3[1], in the following process/activity oriented regulations are presented, comprising the actions/roles and interactions of the various stakeholders participating in the Cross-CPP Ecosystem. The key aspect driving the required regulation is the GDPR (General Data Protection Regulation)[2] approved by the European Parliament, the Council of the European Union and the European Commission. It protects people's personal data throughout the European Union (EU). The decree also affects data exports from the EU.

The General Data Protection Regulation enforces rules that protect people against a wide variety of privacy issues. It enforces the right for people to lawfully agree with companies to use their private information. It also enforces the right for people to have their private information no longer accessible by a company. It enforces that users have the right to allow their private information to become public or not. The regulation also makes sure that no personal data is processed unless the user has allowed the processor of personal data to do so.

The GDPR is aimed at giving citizens control over their personal data. Hence, as outlined in D1.3[3] in the scope of Cross-CPP the following regulations have to be declared, addressing the interaction between the various stakeholders of the Cross-CPP Ecosystem:

---

[1] D1.3 Public Innovation Concept

[2] European Parliament and Council of the European Union, „Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", Official Journal L 119 of 4.5.2016, 1, 2016

[3] There are other directives which also covers personal data transfer/protection, in particular:

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - COM/2017/010 final available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

- Contractual Regulations between the key stakeholders
- Privacy /Security Issues

Furthermore, the two main data models of the Cross-CPP Ecosystem the

- CIDM Standard as the brand independent format for the data exchange in the Cross-CPP Ecosystem and
- Context Model

have to be updated, because these data models have living formats which might require adaptations in case the data consumer are asking for additional signals/channels or extended context information needed for their services. Therefore, a respective regulation update is required.

The key stakeholders of the Cross-CPP Ecosystem value chain and their relationship are presented in Figure 1. In the order of the data flow these are:

- The CPP Owner represents the owner of the collected data during the operation of the CPP.
- The CPP Manufacturer is harvesting the CPP signals and after some proprietary to a non-proprietary data transformation and preprocessing activities he forwards the data to the CPP cloud storage vault in the CIDM standard format.
- The Cloud Storage Provider stores the received data in a self-contained storage vault for each CPP owner the data belong to.
- The Marketplace Operator, as the one-stop-shop access point, represents the mediator between the data of the various CPP Owners and the Service Providers (data consumers). The Marketplace will also offer a Data Analytics Toolbox and a Context Sensitivity Service providing easy to use big data analytic functionalities and context supported functionality to Service Providers.
- The Service Provider is the data consumer who, based on the data from the various CPP Owners, creates B2B and B2C services and offers these to their customers.
- Furthermore, there is a Standardization Board required to update the CIDM standard format in respect to changing market needs of data consumers. This Board consists of representatives of the CPP manufacturer and the Marketplace.

COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy. {COM(2017) 9 final}, 10.01.2017, available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy

COMMISSION STAFF WORKING DOCUMENT Guidance on sharing private sector data in the European data economy {COM(2018) 232 final} available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy
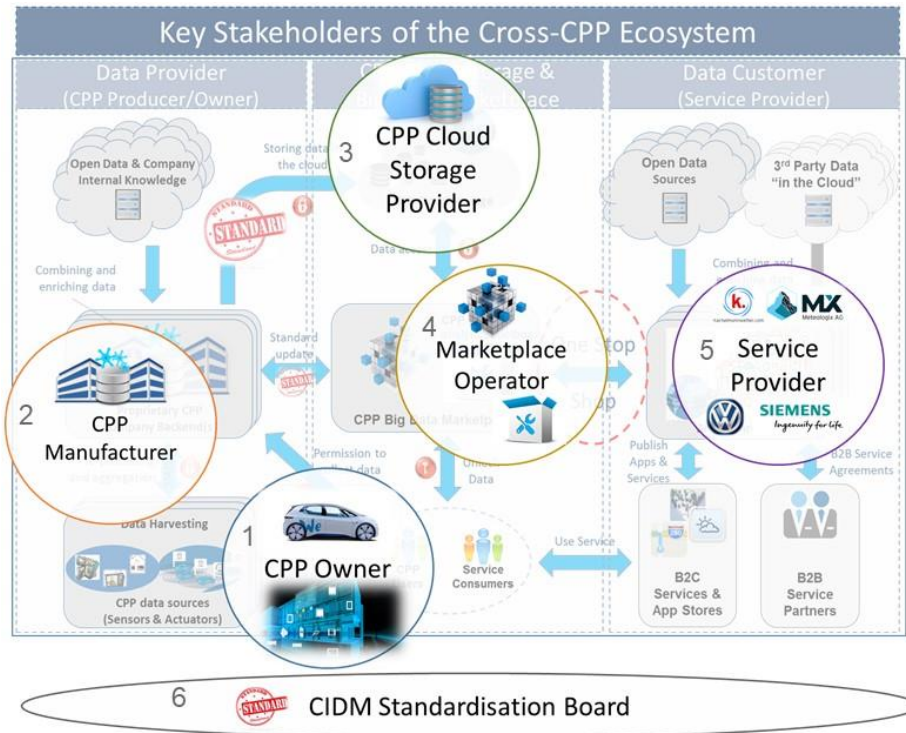
Figure 1: Key Cross-CPP Ecosystem Stakeholder

3. Contractual Regulations

As already outlined above, the GDPR is aimed at giving citizens control over their personal data. This causes the necessity to formulate contractual regulations for the interaction between the various stakeholders of the Cross-CPP Ecosystem guaranteeing the citizens control over their personal data. This requires the following contractual regulations between data owner and respective stakeholders:

- CPP data owner and CPP Manufacturer
- CPP data owner and Cloud Storage Provider
- CPP data owner and Marketplace Provider
- CPP data owner and Service Provider (data customer)
- CPP data owner and Provider of the Marketplace Services (Analytics Toolbox & Context)

The Marketplace represents the "One-Stop-Shop", the single point of entry for a brand-independent access for Service Providers to retrieve data streams from multiple cyber-physical mass products. The Marketplace is the meditator for all the actors involved in the flow of the data in the Cross-CPP Ecosystem. Thereby, the Marketplace knows which stakeholders are participating in the Cross-CPP Ecosystem, which data from which data owner are harvested by which CPP Manufacturer and used by which Data Consumer. In this respect, the Marketplace, in turn, will maintain the mapping between CPP Owners (e.g. CPP_ID, which signals/channels), CPP Manufacturer (e.g. ID, data forwarded storage vaults), Storage Providers (e.g. ID, CPP Owner ID, data available) and Data Consumer: (e.g. registration, data request, data Owner access right).

This central stakeholder interaction management by the Marketplace represents the basic concept of the Cross-CPP Ecosystem in order to carry out the access control of the CPP Owner's data by the various data consumers at run-time, as well as being able to answer accurately future requests by any Service Provider.

3.1. Data Harvesting Agreement

In the following section the regulations are presented to guarantee that the CPP Owner has full control of the data harvested from his CPP. For this, the CPP owner has to give the permission to the CPP Manufacturer to collect the available CPP data and to pre-process them. The arrangement of this contractual agreement must be driven by the CPP Manufacturer, because only he knows which signals of the individual CPP are available to be forwarded to the outside world. Furthermore, the CPP Owner has to agree that the CPP Manufacturer forwards his data to a cloud storage vault (location to be decided at agreement point).

Action/Topic	**Regulation**
Regulation topic	This regulation applies to the process that the CPP Manufacturer gets the CPP owner's permission to gather, pre-process and forward data to his storage vault in the cloud.
Stakeholders Affected	The stakeholders addressed by the data harvesting related regulations are: • CPP Owner • CPP Manufacturer • Big Data Marketplace Provider • Storage Provider
Registration	A CPP owner has to register as a data provider at the Marketplace and the CPP Manufacturer has to be informed. A CPP Manufacturer who intends to participate in the Cross-CPP Ecosystem to offer data of his CPP Owners to the outside world has to register as a partner at the Marketplace, too.
Access Rights Initialization	A registered CPP Owner needs to give the permission to the CPP Manufacturer to collect which signals/channels under which constraints and to forward these data to be stored in the CPP Owner's Cloud Storage vault. The CPP Manufacturer has to configure the data logger of the respective CPP to harvest the agreed signals/data, adapt the respective preprocessing and to be prepared to forward the CPP data in the CPP-Owner's storage vault in the CDIM format. The contract information has to be forwarded to the Marketplace for the CPP Owner contract registration and management, covering information about CPP Owner, CPP device and harvested CPP data.

Action/Topic	Regulation
Access Rights update	If the CPP owner decides to modify the harvested signals or constraints the access right contract with the CPP Manufacturer must be updated.
	A respective logger adaptation required has to be initiated by the CPP Manufacturer and the Marketplace informed about the modifications.
Access Rights Termination	In the case that a CPP Owner does not want to provide data any more (for instance, because the vehicle was sold), he can revoke the CPP Manufacturer's data gathering authorization.
	In order to stop data gathering, based on the CPP Owner's request, the CPP Manufacturer has to reconfigure the involved CPP data harvesting configuration so that no data are gathered any more.
	This will trigger in the Marketplace the process of removing the Data Owner from any active data delivery contracts to Service Providers in which he is involved.
	The Storage Provider has to be informed about this termination, as precondition to delete the data Owner's historical data in his storage area.
Implementation examples/alternatives	The implementations for the data harvesting and the communication with the CPP Manufacturer Backend, as well as any pre-processing activities are entirely proprietary solutions of the CPP Manufacturer.
	To set up the permission for the CPP Manufacturer to collect which signals/channels under which constraints a wide spectrum of solution alternatives might be possible such as:
	· Out of a provided list of accredited signals and constraints the CPP Owner directly selects the data allowed to be harvested. · Marketplace supports the selection process · The CPP Manufacturer supports the selection process (e.g. for vehicles the car dealer might supports the CPP owner to set up the harvesting permission during the sales arrangement).
	There is a huge demand for innovative solutions for future extension of the solution.

3.2. Booking of CPP Owner's Storage Vault

In the following the regulations are presented to guarantee that the CPP Owner has full control of the data stored from his CPP. For this, the CPP Owner has to agree with an accredited Cloud Storage Provider to store his CPP data forwarded by the CPP Manufacturer in a CPP Owner's storage vault. Furthermore, the Marketplace has to be informed about this agreement.

Action/topic	Regulation
Regulation topic	This regulation applies to the process that the CPP Owner rents a cloud storage vault for his CPP data forwarded by the CPP Manufacturer.
Stakeholders affected	The stakeholders addressed by the storage related regulations are: • CPP Owner • Storage Provider • CPP Manufacturer • Marketplace
Storage Accreditation	A Cloud Storage Provider targeting to offer data storage vaults in the scope of the CPP Ecosystem has to fulfill a set of mandatory requirements (e.g. interface standard, data transmission security, data access rules etc.). The compliance with the Cross-CPP accreditation criteria has to be controlled by the Marketplace. If the Storage Provider owns such an accreditation he will become part of the Marketplace catalogue and can offer storage areas to any CPP Owner.
Storage Rights Initialization	The CPP Owner chooses a cloud storage vault for his CPP specific data. For this purpose the CPP Owner enters a contract with a Cloud Storage Provider for creating his own cloud storage area. This cloud storage vault represents the private data storage for the CPP Owner, where his data forwarded by the CPP Manufacturer will be stored. The CPP Owner's cloud storage vault has to be registered in the Marketplace. In reference to this contract, the CPP Manufacturer has to be informed to which storage location the data of the CPP owner have to be forwarded.
Storage Rights Termination	The CPP Owner can at any time resign to store his data in his cloud storage vault. The termination process is also triggered when the owner intends to revoke his data gathering agreement with the CPP Manufacturer (e.g. car is sold). In this case the Storage Provider has to delete the data Owner's historical data in his storage area. The Storage Provider has to inform the Marketplace that the storage vault is not accessible anymore. This triggers the update of the Marketplace's list of active data vaults and CPP Owners. Furthermore, the CPP Manufacturer has to be informed to stop the data transfer activity.

Action/topic	Regulation
Implementation examples/ alternatives	Any institution with a respective storage infrastructure may apply for an accredited Storage Provider such as the CPP Manufacturers, Banks etc.
	There is also a wide spectrum of alternatives to support CPP Owner in selecting a storage provider, such as:
	• Out of a list of accredited storage provider the CPP Owner directly contacts a storage provider • Marketplace supports the storage provider selection process • For vehicles e.g. the dealer of the CPP Manufacturer might supports the CPP owner storage selection together with the harvesting permission agreement in the scope of the conclusion of the sale arrangement. • etc.
	There is a huge demand for innovative solutions for future extension of the solution

3.3. Data Access Agreement Service Provider

In reference to interaction between CPP Owner and Service Provider, regulations are in place to guarantee that the CPP Owner has full control of the usage of the data from his CPP by any Service Provider. Therefore, for the data the Service Provider would like to have access to, the CPP owner has to give the permission to the Service Provider to use his data for a specific service offered to customers of the Service Provider. Thereby, the Marketplace supports the Service Providers in the form of an easy access and detection of needed data (refer to the Service Provider user guideline for more information). The Marketplace is also involved in the enforcement of the access permission between the CPP Owner and the various Service Providers, an essential pre-requisite for the data access control of the Marketplace at run-time.

Action/Topic	Regulation
Regulation topic	This regulation applies to the process of using CPP Owner data by Service Providers to generate their services.
Stakeholders affected	The stakeholders addressed by the data access related regulations are: • CPP owner • Service Provider • Big Data Marketplace
Registration	Any Service Provider who intends to have access to the data of the CPP Ecosystem has to register as a Data Consumer at the Marketplace.
	To overcome the certification process some requirements are mandatory such as compliance with data protection regulations etc.

Action/Topic	Regulation
Order Release	Based on the information provided by the Marketplace (data catalogue, test data, statistics) the Service Provider has to specify a request (an offer) covering the data he wants to have access to for his services. In reference to the data request, the Marketplace has to check the availability of relevant data sources. The Service Provider has to be informed with regard to the available data sources. In case the Service Provider is satisfied with the number of data sources and their characteristics, he will proceed to place an offer for the selected data.
Access Right Initialization	The Marketplace represents the central point to manage the CPP Owner permissions for the data access by the Service Providers. Generally, the Marketplace forwards the Service Provider offer to the CPP Owners for which data was selected. This approach has to be followed for B2B type services (e.g. local weather information for farmers, generation of route roughness information for civil services etc.) where the Service Providers have no direct contact with the CPP Owner. This B2B type services mostly use anonymized data from a large amount of CPP Owners. As already described above the Marketplace has to identify the respective data owner and forward the data request. If the CPP Owner gives the access permission (accepting the offer), this contract represents the reference for the access control at run-time by the Marketplace. In the B2C type business, where the Service Provider may have direct contact with the CPP Owner an alternative approach feasible. In this case the Service Provider can directly contact the CPP Owner to arrange an access agreement. For instance, when booking the service the CPP Owner directly agrees that the Service Provider has access to his data. In this case, the Marketplace has to be informed about this agreement.
Access Right Update	In case of required updates of data requests by Service Providers the Marketplace has to manage the adaption of the modified data access permissions of the Data Owner. Thus, also the access control at run-time has to be modified.
Access Rights Termination	In order to stop data access, either from CPP Owners side or from Service Provider side the Marketplace has to delete the data access agreement for this CPP Owner/Service Provider relation.
Implementation examples/ alternatives	Even though the access agreement deals with a one-to-one relation between CPP Owner and Service Provider simple time and cost efficient contract arrangement solution are needed (e.g. sending email or newsletters or via webpage or dashboard where CPP Owners can

Action/Topic	Regulation
	search for new offers). There is a huge demand for innovative solutions for future extension of the solution.

3.4. Data Access Agreement Marketplace Services

The Marketplace also offers a Data Analytics Toolbox and a Context Sensitive solution. The toolbox services provide easy to use big data analytic functionalities to support Service Providers with low big data expertise and knowledge. The context sensitive solution enables the use the CPP data on the context under which the data is generated to improve user experience and filter CPP data for provision according to the Service Provider need for the services. As integral part of the Marketplace, these Marketplace Services are offered and can be booked via the Marketplace by any member of the Service Provider community of the Cross-CPP Ecosystem.

As any other Service Providers, also the Toolbox and Context Sensitive solution Providers have to ask the CPP Owner for the permission to use his data for these services. Therefore, also the Marketplace Services have to arrange a contractual agreement with the CPP Owner to guarantee that he has full control over the use of his data.

Action/Topic	Regulation
Regulation topic	This regulation applies to the process of using CPP Owner data by the Marketplace Services (Data Analytic Toolbox and Context Sensitive solution).
Stakeholders affected	The stakeholders addressed by the data access related regulations are: • CPP owner • Provider of the Marketplace Services • Marketplace Provider
Registration of Marketplace Services	Any Toolbox or Context Sensitive solution Provider who wants to offer and operate his service via the Marketplace has to make an agreement with the Marketplace Provider to install the required data access for the respective Marketplace Service, as well as to integrate the service into the user interface and the user guidelines as required for the usage by any external Service Provider.

Action/Topic	Regulation
Access Rights Initialization	For each of the data requests (offers) that want to use the Toolbox and Context Sensitive solution, the Marketplace identifies the corresponding CPP Owners. These owners, will accept (or not) the offer in question (creating the data access agreement), not only for the use of the CPP data but also for the for the access to the CPP data by the Marketplace services at run-time.
Access Rights Update	In case the data requirement of the Marketplace Services change the Marketplace has to manage the adaption of the modified data access permissions of the CPP Owner and also to modify the access control at run-time.
Access Rights Termination	In order to stop data access, either from CPP Owners side or from Marketplace Service Provider side the Marketplace has to delete the data access agreement for this CPP Owner/Marketplace Service Provider relation.
Implementation examples/ alternatives	Just as the arrangement of the access agreement between CPP Owners and Service Providers, also for the agreement between CPP Owners and Marketplace Service Providers simple time and cost efficient contract arrangement solution are needed. There is a huge demand for innovative solutions for future extension of the solution.

3.5. Marketplace Authorization to Broker Owner's Storage Data.

The following regulations guarantee that the Data Owner has full control that a Marketplace Provider is authorized to broker his data. For this, the Data Owner will authorize a Marketplace Provider to access the data in the Data Owner's storage area and to forward them to specific authorized service providers, having a contractual arrangement with the Data Owner to use his data.

The Storage Provider has to be informed which Marketplace Provider has access to the data of a Data Owner. Furthermore, in the scope of the contractual agreement between Service Provider and Data customer regarding the data access (see 6.1.3), the Service Provider has to be informed via which Marketplace Provider he has access to the desired data.

Action/Role	Regulation
Regulation topic	This regulation applies to the process to authorize a Marketplace Provider to access the data in the Data Owner's storage area and to forward them to specific authorized Service Providers

Action/Role	Regulation
Stakeholders affected	The stakeholders addressed by the data access related regulations are: • Data Owner • Marketplace Provider • Storage Provider • CPP Service Provider
Marketplace Offer	Any Marketplace Provider who intends to participate in the Cross-CPP Ecosystem has to offer his brokering services to Data Owners. A Marketplace Provider targeting to offer data brokering services in the scope of the CPP Ecosystem has to fulfill a set of mandatory requirements (e.g. interface standard, data transmission security, data access rules etc.).
Cally. *Marketplace Rights Initialization*	The CPP Owner authorizes a Marketplace Provider to broker his data. For this purpose the CPP Owner enters a contract with a Marketplace Provider that allows the respective Marketplace to have access to the data in the Data Owner's specific data storage area at the respective Storage Provider. Furthermore, the Marketplace Provider will be authorized to forward these data to specific, by the Data Owner authorized Service Providers. In reference to this contract, the Storage Provider has to be informed which Marketplace Provider is allowed to have access to the data of a Data Owner. Furthermore, the Service Provider has to be informed which Marketplace Provider he has to address to get access to the desired data of a specific Data Owner.
Marketplace Rights Termination	The CPP Owner can at any time resign the authorization of a Marketplace Provider to broker his data. The termination process is also triggered when the Data Owner resigns his cloud storage vault with the Storage Provider. In this case the Storage Provider has to delete the data access rights of the respective Marketplace. Also the Service Provider has to be informed that the specific Owner's data cannot be accessed via this Marketplace anymore.
Implementation examples/ alternatives	Any institution with a respective Marketplace infrastructure and services fulfilling a set of mandatory requirements compatible with the Cross-CPP Ecosystem may offer his services to any Data Owner.

4. Privacy/Security Issues

The following the Cross-CPP regulations address privacy/security issues with special reference to the GDPR. The Cross-CPP ICT solution shall allow to adapt the privacy, security ethical rules in the cross sectorial services to the current user's context, based on identified conditions (context) under which the CPP data is being generated.

Action/topic	Regulation
Regulation topic	This regulation applies to the to privacy/security issues of the Cross-CPP Ecosystem
Stakeholders affected	The stakeholders addressed by privacy/security issues: • Marketplace • CPP owner • CPP Manufacturer • Storage Provider • Service Provider • Provider of the Marketplace Services
Reference	General Data Protection Regulation (GDPR) approved by the European Parliament, the Council of the European Union and the European Commission, covering existing laws and regulations governing personal data protection and privacy in the European Union.
Targets	The stated target aims that the CPP Owner can choose whether to share own data with third parties for their commercial purposes based on a contract. Moreover, the data owner must be able to deactivate specific data accesses etc. All these principles require that the data owner always must be aware about 'who is using which data for what purpose', even for the usage of anonymized data by a Service Provider. Furthermore, a secure data communication between the various stakeholders of the Cross-CPP Ecosystem has to be guaranteed.
Privacy by Design	'Privacy by design' and 'privacy by default' has to become an essential principles in EU data protection rules. This means that data protection safeguards has to be built into products and services from the earliest stage of development and that privacy-friendly default settings should be the norm. The position of Privacy officer should be installed to ensure that regulatory requirements are fulfilled in each one of the components of the Cross-CPP Ecosystem.

Action/topic	Regulation
Personalized /Anonymization Data	In general, the Cross-CPP Ecosystem supports the provision of CPP Owner data for services based on personalized or anonymized data.
	In the case of individual services based on personalized data, the access agreement has to allow the Service Provider to retrieve personal details of the CPP Owner. This applies for a wide range of B2C type services based on personalized data (e.g. insurance case).
	Another large group of services is based on anonymized CPP Owner data from a large amount of CPPs. This comprises B2B type services (e.g. weather forecast to farmers) as well as B2C type services (e.g. road fog information for the vehicle drivers). Thereby, in reference to the data flow in the Cross-CPP Ecosystem the anonymization should happen as early as possible. However, to guarantee to the CPP Owner full control of the usage of his data in case of the Cross-CPP Ecosystem the anonymization can be first realised at the Marketplace before forwarding the CPP data to Service Providers.
Data Security	For the secure data exchange between the various stakeholders of the Cross-CPP Ecosystem encryption/decryption technologies have to be applied.
	The data storage has to ensure the trustworthiness of the data source, protect the privacy of the data owners, prevent data from unauthorized manipulation and ensure data quality.
	The Manufacturer Backends have to mask CPP data following the privacy rules that are defined by each CPP Owner.
	The Marketplace have to ensure that Service Providers' requests do not break the desire of the CPP Owner.
	The Marketplace have to check the integrity and completeness of the data to avoid providing damaged or corrupted data to Service Providers.
	Device data requests may contain a field to denote that personal information is not required. In these cases, the Marketplace only forward anonymous data.
Implementation examples/ alternatives	For the encryption/decryption activities for the data exchange between the various stakeholders of the CPP Ecosystem there are various commercial tools available, e.g Bdrive, tresorit.

5. CIDM Update Regulations

The Common Industrial Data Model (CIDM) Standard represents a living format which might require adaptations in case the data consumers are asking for additional signals/channels needed for their services. In the following the regulations and the involved stakeholders are described for the CIDM update procedure.

Action/Topic	Regulation
Regulation topic	This regulation applies to the processes and activities addressing the update of the CIDM Standard
Stakeholders affected	The stakeholders involved in the CIDM update process are representatives of: • Big Data Marketplace • CPP Manufacturer • CPP Standardization Board Thereby, the Marketplace takes the role as central point for the CIDM management.
CPP Standardization Board	The CPP Standardization Board has to be constituted by representatives of the participating CPP Manufacturers, chaired by a representative of the Marketplace.
Collection of Update Requests	The Marketplace has to collect CIDM update requests forwarded by Service Providers asking for data not yet provided by CPPs. This requires an extension of the actual version of the CIDM by additional signals/channels. The collected update requests have to be forwarded to the Standardization Board. Tailored to suit the market needs a date for a Standardization Board meeting has to be agreed to decide on potential CIDM updates.
CIDM Update Decision	In respect to market needs and business aspects the Standardization Board has to decide which of the Service Provider requests will be accepted and an updated version of the CIDM will be agreed. The Board has to define regulations for the permission of the CPP Owners in respect to the extended CDIM data harvesting and usage. A CIDM update is accepted if 2/3 of the CPP members vote for. However, none of the CPP Manufacturer is explicitly forced to provide the additional signals/channels.
CIDM Update Stakeholder Actions	The marketplace has to forward the updated CIDM to all affected stakeholders of the Cross-CPP Ecosystem, such as: • CPP Manufacturers

Action/Topic	Regulation
	• Storage Providers • Service Providers • Provider of the Marketplace Services The Marketplace has to update the catalogue presented to the data consumer. If the CPP Owner agrees, the CPP-Manufacturer Backend has to update their data logging, enabling the harvesting of the new signal/channels to be forwarded to the storage area. The Storage Provider has to update the internal CIDM data representation of the data owner's storage area in respect to the agreed access rights between CPP Owner and CPP Manufacturer to guarantee that the new CIDM data structure is stored properly.

6. Context Model Update Regulations

The Context Model represents a living format which might require adaptations in case the data consumer are asking for additional filters for the CPP data. In the following the regulations and the involved stakeholders are described for the Context Model update process.

The definition of the context (context modelling) allows for time and cost effective extensions with additional data sources, rules and CPP from various sectors

The context Models have to be specific for various CPP and sectors. However, in order to gain efficiency in model definition, generic context models are defined which that can be adapted to the specific CPP/sector. Therefore, the context model includes generic, sector and CPP specific concepts so that it will be extensible for different sectors and industrial areas.

The context Models have to be specific for various CPP and sectors.

Action/Role	Regulation
Regulation topic	This regulation applies to the processes and activities addressing the update of the Context Model.
Stakeholders affected	The stakeholders involved in the Context Model update process are representatives of: • Marketplace Provider • Context Model Provider

Action/Role	Regulation
Collection of Update Requests	The Marketplace collects context related filters update requests forwarded by the Service Provider asking for filters not yet provided by the Context Sensitive solution. This requires an extension of the current version of the Context Model and/or associated reasoning rules (refer to the Marketplace developer guide for more information). The collected update requests are forwarded to the Context Sensitive solution provider.
Context model Update Decision	In respect to market needs and business aspects the Context Sensitive solution provider will decide if and when the requests will be implemented. However, the Context Sensitive solution provider is not explicitly forced to provide the additional CPP data filters.
Context model Update in the Stakeholder Action	Once the Context model and/or new rules for CPP Data filtering, the Marketplace presents the updated CPP Data filtering options to the Service Providers and future data filter is presented to the Service Providers.

7. FAQ

For any questions or inquiries about the use of the Cross-CPP Ecosystem or the contents of it or this guidelines, please forward it to: general-support@cross-cpp.eu.

Q: What methodologies are covered by this guide?

A: The presented methodology guidelines cover legal, privacy and consent regulations for key processes/activities in respect to the actions/roles of the various stakeholders and their interaction required for the operation of the Cross-CPP Ecosystem.

Q: As an interested stakeholder, which contractual regulations do I have to take into account?

A: There are methodologies for different kind of contractual regulations addressing different stakeholders of the ecosystem. More information about which regulations are affecting each stakeholder can be found in chapter 3.

Q: Do you also consider privacy and/or security issues regulations?

A: The Cross-CPP ICT solution shall allow to adapt the privacy, security ethical rules in the cross sectorial services to the current user's context, based on identified conditions (context) under which the CPP data is being generated. More details about this are in chapter 4.

8. Glossary

Administrator: Cross-CPP marketplace system administrator

AEON: AEON application

AEON application: publication/subscription based communication application

AEON channel: set configuration for communication between two actors through AEON application

Cross-CPP: System

Analytics Toolbox: set of available analytics functions to be requested by the Data Consumer

Channel: sampler of the data the signals process

CIDM: Common Industrial Data Model

CIDM model: standardized data model for industrial data-driven services

Contract: entity that resumes the acceptance of a data request from a data owner

CME: Context Monitoring and Extraction module

CPP: cyber-physical product

CPP Data: data created by a CCP and sent to the system by the Data Provider

CPP Owner: Data Owner which CPP is registered in the Cross-CPP data-marketplace

Data Consumer: actor who receives the data created by owners to use it on the creation or improvement of services

Data Consumer Wallet: group of MP functionalities for Data Consumers

Data Owner: owner of the CPP that sends data to the system

Data Provider: OEM that provides its users data to the Cross-CPP marketplace

Data Request: set of configurations that define a scope for CPP Data to be received by a Data Consumer

Marketplace: Marketplace Web Application

My Data Wallet: group of MP functionalities for Data Owners

MP: Marketplace

OEM: Original Equipment Manufacturer

Offer: published and available Data Request

Provider: Data Provider

Service Provider: Data Consumer

Signal: information provider of the data the CPP sensors generate

System: the whole lot of applications that conforms Cross-CPP, including Marketplace Web Application and Marketplace Server.

Figures

Build innovative
services upon
cross-sectorial data
streams
The future is connected

About Cross-CPP

The objective is to establish an IT environment for the integration and analytics of data streams coming from high volume (mass) products with cyber physical features, as well from Open Data Sources, aiming to offer new cross sectorial services and focusing on the commercial confidentiality, privacy and IPR and ethical issues using a context sensitive approach. The project addresses cross-stream analysis of large data volumes from mass cyber physical products (CPP) from various industrial sectors such as automotive, and home automation. The business objective of the research is to allow for analyses of such data streams in combination to other (non-industrial, open) data streams and for the establishment of diverse enhanced sectorial and cross-sectorial services. The project will develop: (i) New models for integration and analytics of data streams coming from multi-sectorial CPP, including shared systems of entity identifiers applicable to multi-sectorial CPP (as well as the definition of agreed data models for data streams from multiple CPP aiming at defacto standard; (ii) Ecosystem, including a common Marketplace, and methodology to use such models to build multi-sectorial cloud based services, (iii) Toolbox for real-time and predictive cross-stream analytics, context modelling and extraction, and dynamically changing security policy, privacy and IPR conditions/rules and (iv) set of services such as services based on a combination of data streams from home automation and (electrical) vehicles to pro-vide enhanced local weather forecast and predict and optimise energy consumptions in households. The project will build upon the results from past and current projects, where results from the project AutoMat, addressing services developed based on data streams from vehicles, will be used as a basis for further development aiming to extend it to integrated, cross-sectorial data streams analytics. More information is available at https://cross-cpp.eu